**3GPP TSG-SA3 Meeting #119 draft\_S3-245184-r5**

Orlando, USA 11-15 November 2024 *revision of S3-244723, merger of S3-244610, S3-245081*

**Source: US National Security Agency, OTD\_US, Johns Hopkins University APL, MITRE-FFRDC, Ericsson, Motorola Mobility, Nokia, Nokia Shanghai Bell**

**Title: General Recommendations for Conclusion 2 Policy Enforcement**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***It is proposed to approve the proposed changes to TR 33.794 clause 8.2 conclusions for KI 2***

# 2 References

[8] NIST Special Publication 800-207: "Zero Trust Architecture".

# 3 Rationale

This submission provides additions to conclusion 2 including some general recommendations.

# 4 Detailed proposal

\*\*\*\*\*Start Changes\*\*\*\*\*

8.2 Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA

No normative work is needed for KI#2.

Informative guidance for this KI includes the following aspects:

For security policy enforcement and improved access control decisions, security evaluation and monitoring results are described as follows:

1. A Policy Enforcement Point (PEP) in SBA performs actions based on security evaluation results/outcome (e.g., in case of NF being identified/suspected to be compromised) during NF service requests (e.g., NF service discovery, access token requests, NF service update) and there may be more than one PEP within the SBA.
2. NF (i.e., service producer or service consumer) acts as PEP (i.e., in case of deployment A when no NRF and SCP involved as well as in general case of SBA service request/response as applicable)
3. NRF acts as PEP (i.e., in case of deployment B where NRF is involved).
4. NRF and SCP acts as PEPs (i.e., in case of deployment C first NRF is involved in Service discovery and then SCP is involved during service request).
5. SCP acts as a PEP (i.e., in case of deployment D).

NOTE 1: Communication models for NF/NF services interaction are described in TS 23.501 [18].

1. If SBA NF performs PEP functions (e.g. as described in NIST [8]) then following actions are needed:
2. The PDP instructs the PEP i.e., actions to the NF functioning as a PEP.

NOTE 2: PDP decides on the security issues/incidents and how the related responses were decided is left to MNO’s implementation. It is upto the MNO to decide the security issues and the corresponding responses.

1. PEP takes actions according to (2.a).

\*\*\*\*\*End Changes\*\*\*\*\*